Order Code RL32840

CRS Report for Congress
Received through the CRS Web

Border and Transportation Security: Selected Programs and Policies

March 29, 2005

Lisa M. Seghetti, Jennifer E. Lake, and William H. Robinson
Domestic Social Policy Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
29 MAR 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Border and Transportation Security: Selected Programs and Policies	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Repository Defense Acquisition University Fort Belvoir, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**28**	

Border and Transportation Security: Selected Programs and Policies

Summary

Border and Transportation Security (BTS) is a pivotal function in protecting the American people from terrorists and their instruments of destruction. This report addresses selected programs and policies now in place that seek to attain higher levels of BTS. It is the second in a three-part series of CRS reports that make use of analytical frameworks to better understand complex phenomena and cast them in terms that facilitate consideration of alternative policies and practices. (The first report in the series, CRS Report RL32839, *Border and Transportation Security: The Complexity of the Challenge*, analyzes the reasons why BTS is so difficult to attain. This report is the second in the series. The final report is CRS Report RL32841, *Border and Transportation Security: Possible New Directions and Policy Options*.)

Congressional concern with terrorism and border security was manifested as early as 1993, with the first World Trade Center attack and subsequent terrorist attacks against U.S. targets abroad. The congressional response to these events began with attempts to understand the nature of the terrorist threat through the creation of several commissions. The response to the 9/11 attacks was followed by specific, targeted measures to protect the nation such as the creation of the Transportation Security Administration and the passage of laws that were aimed at strengthening security at the border, including immigration policies with respect to the admission of foreign nationals; and strengthening security in the maritime domain. Congressional interest continues in more comprehensive approaches including recent efforts to respond to the report of the 9/11 Commission.

There are several broad strategies that could be pursued to enhance border security. Current programs and policies can be grouped under the following generic categories, which include pushing the border outwards to intercept unwanted people or goods *before* they reach the United States (as in the passenger pre-screening program); hardening the border through the use of technology (as shown by biometric identifiers); making the border more accessible for legitimate trade and travel (as in "trusted traveler" programs); strengthening the border inspection process through more effective use of intelligence (with the integration of terrorist watch lists); and multiplying the effectiveness of interdiction programs through the engagement of other actors in the enforcement effort (as displayed by bi-national accords with Canada and Mexico). It is also possible to use the strategies as a checklist for what new efforts might be explored.

Many current programs and policies to enhance border and transportation security were put into place as a result of the 9/11 terrorist attacks with a sense of urgency — *to prevent another attack*. Programs and policies in existence prior to the attacks, however, were often created with a different focus and not necessarily with the terrorist threat in mind. The challenge for Congress is to review these programs and policies comprehensively to help them form a more coherent and effective overall strategy. This report will be updated periodically as events warrant.

Contents

List of Figures

Border and Transportation Security: Selected Programs and Policies

Introduction

Border and Transportation Security (BTS) is a pivotal function in protecting the American people from terrorists and their instruments of destruction. While BTS may be difficult to attain, the federal government has put into place multiple programs and policies to achieve this goal. The three reports in this series attempt to provide an understanding of the complex problems faced in seeking enhanced border and transportation security, suggest a framework to better understand existing programs and policies, and explore some possible new directions and policy options.

As noted in the first report[1] in this series, homeland security efforts can be seen as a series of concentric circles or screens, with the outer screen being that of preventive efforts launched *outside* the country — before terrorists or their weapons can reach the country. The continuum of activities to provide homeland security then moves through progressively smaller circles starting from more distant efforts to closer and more localized measures, ending with emergency preparedness and response. Thus, the process starts with prevention abroad and progresses through the other stages as needed.

As the first report in this series observes, border management is a complex task and current programs and policies in place to strengthen the border and facilitate the flow of legitimate people and things can seem overwhelmingly complex and difficult to approach in a systematic way. This report addresses the myriad programs and policies that make up the nation's current approach to attaining higher levels of BTS. Before doing so, however, it is useful to review the development of congressional concern and policy approaches.

Congressional Concerns

Congressional concern with terrorism and border security was manifested early, following a series of terrorist attacks beginning in the 1990s. The shock of the first World Trade Center attack in 1993 was followed by two attacks in Saudi Arabia (Riyadh in 1995 and Khobar Towers near Dhahran in 1996), the simultaneous Embassy bombings in 1998 (Kenya and Tanzania), the attack on the USS Cole in 2000, and culminating in the catastrophic attack on the World Trade Center and the Pentagon on September 11, 2001. The congressional response began with inquiries related to the nature of the terrorist threat, and was followed by specific, targeted

---

[1] CRS Report RL32839, *Border and Transportation Security: The Complexity of the Challenge*, by Jennifer E. Lake, William H. Robinson, and Lisa M. Seghetti.

measures to protect the nation following the events of 9/11. There are indications that congressional interest continues in broader, more comprehensive approaches including recent efforts to respond to the report of the 9/11 Commission contained in the National Intelligence Reform Act of 2004 (P.L. 108-458). Congressional policy evolution is charted briefly below:

- *Broad efforts to understand the terrorist threat* — Starting in 1998, Congress created three commissions to better understand the nature of the terrorist threat facing the nation. These included the Gilmore Commission (to investigate domestic preparedness to cope with weapons of mass destruction), the Bremer Commission (to explore the terrorist threat and what could be done to prepare for it), and the Hart-Rudman Commission (to investigate national security challenges in the 21st Century).[2]
- *Structural changes to provide a proper framework for action* — Following the 9/11 attacks, Congress enacted legislation to create the Department of Homeland Security to provide a structural framework for subsequent action, and the USA PATRIOT ACT to provide the tools needed for the new challenge to national security.[3] Starting even earlier, but continuing through this period, Congress attempted to remedy perceived flaws in the immigration system with a series of legislative measures.[4]
- *Highly specific actions to protect against immediate threats* — Understandably, following the 9/11 attacks that were committed by foreign national extremists, early legislative action called for the immediate implementation of the entry and exit control system, the use of biometric identifiers in travel documents, and intelligence sharing among federal law enforcement and immigration agencies through the passage of the PATRIOT Act. Airline security measures were taken with the creation of the Transportation Security Administration, among other things in the Aviation and Transportation Security Act. That was soon followed by the Enhanced Border Security and Visa Entry Reform Act to tighten immigration practices and tools, and legislation to protect against the

---

[2] The official names and dates of creation of the Commissions are as follows: (1) Gilmore Commission, known officially as *The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction,* created on Oct. 17, 1998 (P.L. 105-241); (2) Bremer Commission, known officially as *The National Commission on Terrorism*, created on Oct. 21, 1998 (P.L. 105-277); and (3) Hart-Rudman Commission, known officially as *The U.S. Commission on National Security/21st Century,* created on Sept. 2, 1999.

[3] The USA PATRIOT Act, known officially as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 was passed on Oct. 26, 2001 (P.L. 107-56). The Homeland Security Act was passed on Nov. 25, 2002 (P.L. 107-296).

[4] See for example the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (P.L. 104-208).

serious threats posed in the maritime domain with enactment of the Maritime Transportation Security Act.[5]

- *Interest in broader, more comprehensive approaches* — As evidenced in recent oversight hearings, Congress has been frustrated by the failure to more aggressively address other border and transportation security threats (including the need to create integrated terrorist watch-lists, and measures to address other modes of transportation — rail and mass transit, air cargo, trucking, and buses). These concerns were given a strong impetus by the Final Report of the 9/11 Commission, which highlighted the need for more strategic approaches to the terrorist threat, and are expressed in legislative form in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458).[6]

The next section of the report traces the development of selected programs and policies designed to achieve higher levels of border and transportation security, and presents them in a framework that facilitates a better understanding of current approaches and some possible new directions.

Selected Programs and Policies

Since the September 11, 2001 terrorist attacks, the nation has made securing the homeland its primary objective. Border security has emerged as a critical stage in achieving this goal. Prior to the terrorist attacks, federal agencies involved in securing the homeland were fragmented and often plagued by internal performance problems. As discussed below, many federal agencies tasked with securing the nation's borders did not communicate with one another. Moreover, technology was inadequate for communications within many of these agencies as well as between agencies. For example, immigration systems and databases, which are critical when trying to determine the admissibility of a foreign national and keep bad people out of the country were not (and to some extent still are not) integrated. In an effort to address some of these issues, Congress passed the Homeland Security Act of 2002 (P.L. 107-296).[7]

The Homeland Security Act of 2002 consolidated many of the federal agencies responsible for border and transportation security into a single department. Within the Department of Homeland Security (DHS) is a Directorate of BTS, which is

---

[5] The Aviation and Transportation Security Act (ATSA, P.L. 107-71) signed on Nov. 19, 2001; the Enhanced Border Security and Visa Entry Reform Act (P.L. 107-143) signed on May 14, 2002; and the Maritime Transportation Security Act of 2002 (P.L. 107-295) signed on Nov. 25, 2002.

[6] See *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington: GPO, 2004).

[7] Congress also passed several other pieces of legislation relevant to Homeland Security — the USA PATRIOT Act; the Enhanced Border Security and Visa Entry Reform Act of 2002; the Aviation and Transportation Security Act; the Air Transportation Safety and System Stabilization Act; and the Maritime Transportation Security Act of 2002.

charged with securing: the borders; territorial waters; terminals; waterways; and air, land and sea transportation systems of the United States. BTS houses the Bureau of Customs and Border Protection (CBP), the Transportation Security Agency (TSA) and Immigration and Customs Enforcement (ICE). Within CBP are the inspections service of the former Immigration and Naturalization Services (INS), the U.S. Border Patrol, the inspections service of the U.S. Customs Service, and the border-related inspection programs of the Animal and Plant Health Inspection Service (APHIS). In addition to the border security-related functions of the former INS and U.S. Customs Service being transferred to CBP, the following agencies were also transferred to DHS: (1) U.S. Coast Guard; (2) TSA; and (3) immigration investigations, intelligence, interior enforcement and detention and removal functions of the former INS and U.S. Customs investigations and interior enforcement. The Coast Guard was transferred to DHS as a stand-alone agency and TSA was maintained in DHS' BTS as a distinct entity.[8]

This section focuses on current border security activities of CBP,[9] the Coast Guard and the airline security component of the TSA. The activities discussed in this section are divided into categories of *how* they provide BTS and further divided into people and goods security-related programs.

Background

The DHS is the primary federal agency responsible for securing the border. CBP's function is to secure U.S. borders while facilitating the legitimate flow of people and goods across the border. CBP personnel carry out these duties by inspecting people and goods prior to entry into the United States and by dispatching border patrol agents to patrol the border *between* ports of entry to prevent people from illegally entering the country. In addition to the various components in DHS, the Coast Guard aids in securing U.S. ports and waterways. In securing the ports and waterways, the Coast Guard performs the following functions: (1) defense readiness; (2) drug interdiction; (3) migrant interdiction; and (4) law enforcement-related functions.[10] Another component of border security is securing the nation's air system, which is primarily done by TSA. Current policies at the border can be separated into two major categories: people-related border security and goods-related border security.

---

[8] According to the Homeland Security Act of 2002 (P.L. 107-296), however, TSA is only required to be maintained as a distinct entity within DHS for two years, until 2004. At the time of this report, TSA was still an independent entity in DHS.

[9] CBP also has an Office of International Affairs (OIA) that is responsible for: managing CBP's international activities and programs; conducting CBP's bilateral and multilateral relations with foreign agencies; overseeing the negotiation and implementation of CBP's agreements with foreign agencies; and managing all foreign training assistance programs provided by CBP.

[10] See CRS Report RS21125, *Homeland Security: Coast Guard Operation — Background and Issues for Congress*, by Ronald O'Rourke.

People-Related Border Security

Since the terrorist attacks, considerable focus has been placed on the fact that the 19 terrorists were aliens who apparently entered the United States legally despite provisions in immigration law that could have barred their admission.[11] Fears that lax enforcement of immigration laws regulating the admission of foreign nationals into the United States may continue to make the United States vulnerable to terrorist attacks have led many to call for tighter measures at the border (as well as during the screening process for visas). These concerns, which are constantly weighed with efforts to facilitate the legitimate travel of people across the border, have been expressed frequently in a legislative form.[12]

Goods-Related Border Security

The U.S. maritime system consists of more than 300 sea and river ports with more than 3,700 cargo and passenger terminals, with most ships calling at U.S. ports being foreign-owned. Container ships have been the focus of much of the attention on seaport security due to the potential of terrorists infiltrating them. More than 6 million marine containers enter U.S. ports each year and while all cargo information is analyzed by CBP officers for possible targeting for closer inspection, only a fraction is actually physically inspected.[13] CBP works in tandem with the U.S. Coast Guard at sea ports of entry. Efforts such as the Coast Guard's requirement that ships provide a 96-hour Notice of Arrival and CBP's Container Security Initiative (CSI) program aid in preventing more harmful things from getting to the United States.

In addition to maritime security, much attention has been focused on the nation's air, truck and rail system. Similar to the massive volume of containers entering the nation's seaports, airports also experience large volumes of cargo.

Current Policies at the Border

The U.S. government has employed a number of strategies and programs to make the nation's borders more secure. The following actions are set in a framework that suggests types of possible policy actions:

- Pushing the border outwards to intercept unwanted people or goods before they reach the United States;

---

[11] Although the 9/11 terrorists appeared to have entered the country legally, it was later determined that some of the terrorists used fraudulent documents and many of them subsequently violated immigration law.

[12] See, for example, the USA PATRIOT Act; the Enhanced Border Security and Visa Entry Reform Act of 2002; and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

[13] See CRS Report RL31733, *Port and Maritime Security: Background and Issues*, by John Frittelli.

- Hardening the border through the use of technology and the presence of more agents at the border;
- Making the border more accessible for legitimate trade and travel;
- Strengthening the border through more effective use of intelligence; and
- Multiplying effectiveness through the engagement of other actors in the enforcement effort (including engaging Canada, Mexico, state and local law enforcement resources, and the private sector).

Efforts to Push Out the Border

Many contend that the best way to secure the border is by addressing issues before they reach the border. While this concept is not new, greater emphasis has been placed on "pushing the border out" since the terrorist attacks. (The following discussion is organized to highlight activities that target people and goods for inspection).

People[14]

In 2004, there were more than 427 million travelers who were inspected at a U.S. port of entry.[15] Of the 427 million travelers who sought entry into the United States in 2003, approximately 62% were foreign nationals. While the majority of travelers seeking entry into the United States are admitted during primary inspections,[16] a small percentage of travelers (less than one percent) are referred to secondary inspections.[17] In theory, by pushing out the border, the number of travelers needing closer scrutiny at the border (i.e., referrals to secondary inspection) would diminish, which would create a higher level of security. Following are a few examples of either congressional mandates and/or administrative initiatives that are aimed at pushing out the border.

Pre-Inspections. Pre-inspections are immigration inspections conducted at foreign ports of embarkation by United States authorities for passengers seeking entry

---

[14] For additional information on immigration inspections, see CRS Report RL32399, *Border Security: Inspections Practices, Policies, and Issues*, Ruth Ellen Wasem, Coordinator.

[15] Preliminary data for FY2004 shows the number of people inspected at a U.S. POE was 433 million. See [http://uscis.gov/graphics/shared/aboutus/statistics/msrsep04/INSP.HTM].

[16] Primary inspection is the first level of inspection and consists of a brief interview with a CBP inspector, a cursory check of the traveler's documents and a query of the Interagency Border Inspection System (IBIS), which is an immigration data system that interfaces with other federal immigration and law enforcement data systems.

[17] A traveler is referred to secondary inspections if the CBP inspector is suspicious that the traveler may be inadmissible under the Immigration and Nationality Act or in violation of other U.S. laws. During secondary inspections, travelers may be questioned extensively and travel documents are further examined. Several immigration databases are queried as well, including "lookout" databases for terrorists.

into the U.S. Congress first authorized immigration pre-inspections in 1996.[18] However, efforts to preinspect travelers had previously been underway for several years. As of spring 2005, 15 foreign airports participated in the pre-inspection program,[19] and Congress has mandated that preinspections be extended to "at least 25 foreign airports."[20]

Under the pre-inspection program, the Secretary of Homeland Security details immigration officers to foreign airports. While immigration officers that are located at pre-inspection sites can perform general inspection functions, other law enforcement functions performed by immigration officers within the United States may be limited in the countries where pre-inspection sites are located.[21]

Although the original intention of pre-inspections was to decrease the number of inadmissible aliens entering the United States, some officials now view it as a useful means to better secure our borders while facilitating the flow of travel. Setting up pre-inspection sites at foreign airports, however, is not without controversy. In order to have a pre-inspection site at a foreign airport, the United States must enter into diplomatic negotiations with the host country. These negotiations include addressing issues such as sovereignty and the extent to which immigration officers can enforce United States' immigration laws in the foreign country. Another issue in setting up pre-inspection sites at foreign airports is the amount of resources it takes to staff them. Immigration officials are assigned to pre-inspection sites based on the volume of travelers seeking entry to the United States. Thus, countries that may not have the volume of travelers to justify a pre-inspection site may still justify having such a site based on the number of "high risk" travelers.

Advanced Passenger Manifest. Air carriers en route to the United States from a foreign country are required to submit passenger manifests in advance of their arrival at a U.S. port of entry. While inspections are done on U.S. soil, such advance notification alerts the CBP inspectors to which travelers will need closer scrutiny. The manifest is transmitted electronically via the Advanced Passenger Information System (APIS), which is integrated with the Interagency Border Inspection System (IBIS), a component of the US-VISIT program.

---

[18] See Section 123 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (P.L. 104-208).

[19] The following foreign airports participate in the pre-inspection program: (1) Oranjestaad, Aruba; (2) Calgary, Alberta, Canada; (3) Edmonton, Alberta, Canada; (4) Freeport, Bahamas; (5) Hamilton, Bermuda; (6) Nassau, Bahamas; (7) Shannon, Ireland; (8) Toronto, Ontario, Canada; (9) Vancouver, British Columbia, Canada; (10) Victoria, British Columbia, Canada; (11) Winnipeg, Manitoba, Canada; and (12) Dublin, Ireland (see 8 CFR 103.1). Three additional airports have the capability to preinspect travelers who are directly en route to the United States: (1) Guam; (2) Puerto Rico; and (3) the United States Virgin Islands (see 8 CFR 235.5).

[20] See §7210(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458).

[21] For example, immigration inspectors enforce various criminal and administrative statutes, apprehend violators, and adjudicate a variety of applications for various immigration benefits.

TSA and ICE Border Security-Related Activities. TSA and ICE have several programs that have implications for securing the nation's borders but are usually not considered to be directly applicable to border security. These programs are either geared towards pre-screening individuals before they embark on a flight originating in the United States or providing intervention during a flight should an act of terrorism occur.

Computer Aided Passenger Pre-Screening System. Since 1996, the Computer Aided Passenger Pre-screening (CAPPS) System has analyzed ticket purchasing behavior to identify air travelers who may pose a threat. While the TSA maintains that the methods of identifying suspicious passengers under the existing CAPPS program has largely been compromised by information publicly discussed following the terrorist attacks, efforts to create a next-generation passenger risk assessment and pre-screening system (CAPPS II) have been scrapped due to mounting privacy concerns and operational problems. On August 26, 2004, however, TSA announced its plans to test a new passenger pre-screening program, Secure Flight.[22] Under Secure Flight, TSA will be responsible for checking domestic airline passengers' names against terrorist watch lists (see discussion below, "Strengthening the Border Through More Effective Use of Intelligence").[23]

The "No-Fly" and "Selectees" Lists.[24] TSA is mandated by law to maintain a watchlist of names of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety." The watchlist was created in 1990 and was initially administered by the Federal Bureau of Investigations, then the Federal Aviation Administration before TSA finally took over the administrative responsibility. Individuals whose names are on these lists are subjected to additional security measures, with a "no-fly" match requiring the individual to be detained and questioned by federal law enforcement and a "selectees" match requiring additional screening. P.L. 108-458 sets forth procedures for appealing erroneous information or determinations made by TSA with respect to the aforementioned records.[25]

Federal Air Marshal Service. The Federal Air Marshall Service (FAMS) was created as a direct result of the events of the terrorist attacks. It was originally a part of TSA but was moved to ICE by DHS in December 2003. FAMS places plain clothes federal law enforcement agents on board "high-risk" flights either destined to the United States or originating in the United States. In the two-year period following the terrorist attacks, air marshals responded to over 2,000 aviation security

---

[22] See CRS Report RL32802, *Homeland Security: Air Passenger Prescreening and Counterterrorism*, by Bart Elias, William Krouse, and Ed Rappaport.

[23] Passengers on international flights names are already checked against names in the consolidated Terrorist Screening Center's database.

[24] See CRS Report RL32802, *Homeland Security: Air Passenger Prescreening and Counterterrorism*, by Bart Elias, William Krouse, and Ed Rappaport.

[25] See §4012(a) of P.L. 108-458.

incidents, used non-lethal force 16 times, discharged their weapons on three occasions and were involved in 28 arrests or detainments of individuals.[26]

In addition to FAMS, other measures to secure passenger airlines include the hardening of cockpit doors, training and arming pilots who volunteer to be Federal Flight Deck Officers, and the training of flight attendants to handle security threats in the aircraft cabin.

Goods

As discussed above, the massive volume of containers that arrive at U.S. ports each year makes it impractical for CBP to inspect every container. In order to focus its limited inspection resources, CBP has launched several initiatives designed to enhance the targeting of high-risk shipments and securing the entire supply chain from point of origin to final destination. While these initiatives assist CBP inspectors with targeting high-risk containers, thus requiring a physical inspection at the border, they also permit the identification of such containers in advance of their arrival at the border.

Advance Electronic Cargo Manifest Requirement. Cargo inspections are dependent on receiving accurate information in a timely manner in order to execute risk assessment and targeting procedures before shipments reach the border. To give inspectors adequate information and time to perform a risk assessment on arriving cargo shipments, the legacy Customs agency published a rule (known as the 24-hour rule)[27] requiring the submission of certain manifest information to Customs 24-hours in advance of the vessel cargo being laden at the foreign port. Current law required CBP to develop rules concerning the mandatory electronic submission of cargo manifest data.[28] CBP published regulations establishing these rules according to the following time-frames:

- Vessel — 24 hours prior to lading in the foreign port;
- Air — 'wheels up' or four hours prior to departure for the United States (depending upon where the flight originated);
- Rail — two hours prior to arrival in the United States;
- Truck — one hour prior to arrival for shipments entered through the Pre-Arrival Processing System (PAPS) or the Automated Broker

---

[26] U.S. Government Accountability Office, *Federal Air Marshal Service Is Addressing Challenges of its Expanded Mission and Workforce, but Additional Actions Needed*, GAO-04-242, Nov. 2003.

[27] U.S. Department of the Treasury, "Presentation of Vessel Cargo Declaration to Customs Before Cargo Is Laden Aboard Vessel at Foreign Port for Transport to the United States," *Federal Register*, vol. 67, no. 211, Oct. 31, 2002, pp. 66318-66333.

[28] The Trade Act of 2002 (P.L. 107-210), as amended by the Maritime Transportation Security Act of 2002 (P.L. 107-295).

Interface (ABI) and 30 minutes prior to arrival for shipments entered through FAST.[29]

Container Security Initiative. The Container Security Initiative (CSI) program, one of a series of initiatives aimed at securing the supply chain, was initiated by the U.S. Customs Service (now CBP) in January of 2002 to prevent terrorists from exploiting containers entering into the United States. CSI is based on four core elements: (1) developing criteria to identify high-risk containers; (2) pre-screening high-risk containers at the earliest possible point in the supply chain; (3) using technology to pre-screen high risk containers quickly; and (4) developing and using smart and secure containers. Under the CSI program, CBP officers are sent to participating ports where they collaborate with host country customs officers to identify and pre-screen high-risk containers using non-intrusive inspection technology *before* the containers are laden on U.S.-bound ships. Similar to CBP inspectors who conduct pre-inspections at foreign airports, (as discussed above), CBP officers stationed at CSI ports are neither armed, nor have arrest powers. CBP continues to expand CSI to additional foreign ports. As of spring 2005, CSI was at 32 foreign ports.

Customs-Trade Partnership Against Terrorism. The Customs-Trade Partnership Against Terrorism (C-TPAT) was initiated in April 2002 and offers importers expedited processing of cargo if they comply with CBP requirements for securing their entire supply chain. C-TPAT participants benefit from fewer cargo inspections, as membership in C-TPAT reduces a company's overall risk score in the Automated Targeting System (ATS).[30] In order to participate in the C-TPAT businesses must sign an agreement that commits them to the following actions:

- conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by CBP and the trade community;
- submit a completed supply-chain security profile questionnaire to CBP;
- develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines; and
- communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

Once the applicant company has conducted the security self-assessment and submitted the security profile, C-TPAT officials review the security profile to develop an understanding of the company's security practices. C-TPAT officials also gather information regarding the company's trade compliance history and any past criminal investigations. Based upon the results of the review, CBP will work with

---

[29] Department of Homeland Security, Bureau of Customs and Border Protection, "Required Advance Presentation of Cargo Information; Final Rule," *Federal Register*, vol. 68, no. 234, Dec. 5, 2003, pp. 68140-68177.

[30] ATS is a risk assessment used by CBP to target its inspections on high-risk shipments.

the company to address any security concerns discovered during the review, or will further reduce the company's risk score.

Additional efforts to push the border out include the following (see **Appendix A** for a description of each program):

- Carrier Consultant Program (people);
- Immigration Security Initiative (people);
- Known Shipper Programs (goods); and
- North American Perimeter Security (people).

Efforts to Harden the Border Through the Use of Technology

The U.S. northern and southwest borders extend over 6,000 miles, with vast areas of both borders lacking direct surveillance by border patrol personnel. While the northern border, historically, has posed less of a problem than its southwestern counterpart, the terrorist attacks have brought attention to the vulnerabilities that both borders pose. The southwest border, on the other hand, has a longstanding history of illegal migrants attempting to gain entry into the United States as well as individuals attempting to smuggle human beings and drugs into the country. The border patrol has increased its manpower along portions of the border and various types of technology are also being used such as video cameras, ground sensors, radiation detectors, geographic information systems, and physical barriers to provide surveillance at the border.[31]

While critics of the current technological infrastructure contend that its weaknesses pose a security risk, efforts are underway to enhance border technology. Issues such as integrating data systems, sharing intelligence among agencies and departments, having technology that can track the comings and goings of foreign nationals and having technology that can read biometric identifiers are all important to border management.

Additionally, agencies continue to invest in technology that will aid in detecting things that may cause harm, including technology that would detect explosives.[32] For example, inspectors are increasingly using portal scanning devices on commercial vehicles to detect radiation. The border patrol has begun using Unmanned Aerial Vehicles (UAV) in its Tucson Border Patrol Sector as part of its Arizona Border Control (ABC) initiative in an attempt to control the flow of illegal migration

---

[31] See CRS Report RL32562, *Border Security: The Role of the U.S. Border Patrol*, by Blas Nuñez-Neto.

[32] See CRS Report RS21920, *Detection of Explosives on Airline Passengers: Recommendation of the 9/11 Commission and Related Issues*, by Dana A. Shea and Daniel Morgan.

between ports of entry.[33] The border patrol also uses other technology such as ground sensors and video cameras.

In addition, CBP has deployed an array of non-intrusive inspection (NII) technologies at ports of entry to assist inspectors with the examination of cargos and the identification of contraband. Large scale NII technologies include a number of x-ray and gamma ray systems. The Vehicle and Cargo Inspection System (VACIS) uses gamma rays to produce an image of the contents of a container for review by the CBP inspector. The VACIS can be deployed in a stationary or mobile configuration depending on the needs of the port. CBP has also deployed several rail VACIS systems to screen railcars entering the country. Other large scale NII systems include truck x-ray systems, which like the VACIS can be deployed in a either a stationary or mobile configuration; the Mobile Sea Container Examination System, and the Pallet Gamma Ray system. CBP also continues to deploy nuclear and radiological detection equipment in the form of personal radiation detectors, radiation portal monitors, and radiation isotope detectors at ports of entry. Following are selected examples of either congressional mandates and/or administrative initiatives that are aimed at hardening the border.

U.S.-VISIT Program[34]

In 1996, Congress first mandated that the former INS implement an automated entry and exit data system (now referred to as the U.S.-VISIT program) that would track the arrival and departure of every alien.[35] The objective for an automated entry and exit data system was, in part, to develop a mechanism that would be able to track nonimmigrants[36] who overstayed their visas as part of a broader emphasis on immigration control. Following the September 11, 2001 terrorist attacks, however, there was a marked shift in priority for implementing an automated entry and exit data system. While the tracking of nonimmigrants who overstayed their visas remained an important goal of the system, border security has become the paramount concern.

Tracking the entry and exit of most foreign nationals at U.S. ports of entry is not a small undertaking. The massive volume of travelers seeking entry into the United States at one of the 300 land, air and sea ports of entry coupled with the demands such a system would place on port infrastructure makes implementing the system challenging. Nonetheless, implementation of the U.S.-VISIT program began at selected air and sea ports on January 5, 2004, and selected land ports of entry on December 31, 2004.

---

[33] The ABC Initiative is a coordinated effort among federal, state and local agencies to secure the Arizona border and its interior.

[34] For additional information on the U.S. — VISIT program, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, by Lisa M. Seghetti and Stephen R. Viña.

[35] Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (P.L. 104-208).

[36] A nonimmigrant is a foreign national admitted to the United States on a temporary basis.

Biometric Identifiers

Although initially required by Congress in 1996 to curtail the use of fraudulent Mexican Border Crossing Cards (now referred to as Laser Visas),[37] biometric identifiers have received a great deal of attention post 9/11 as the need to positively identify people seeking entry into the United States became paramount. The U.S.-VISIT program, as discussed above, brought national attention to such technology as discussion centered around which type of biometrics (i.e., iris scan, fingerprint, facial photograph, etc.) would be best for the program.

Under current law, travel documents must have a biometric identifier that is unique to the cardholder. In May 2003, the International Civil Aviation Organization (ICAO) finalized standards for biometric identifiers, which asserted that facial recognition is the globally interoperable biometric for machine readable documents with respect to identifying a person.[38] In an earlier report published by the National Institute of Standards and Technology (NIST), it was determined that two fingerprints, as opposed to ten-fingerprints, and a facial photograph "... are the only biometrics available with large enough operational databases for testing at this time."[39] Although NIST set the two-fingerprint standard for identifying one's identity, concern has been raised about the possible limitation two-fingerprints pose for obtaining additional information on a person, such as arrest warrants and criminal history.

Smart Containers

In an effort to secure the supply chain across international boundaries, CBP and select volunteer importers participating in C-TPAT have begun testing a new "smart container." Although increasingly sophisticated tools exist, such as bomb sniffers and high-tech locks, many view smart containers that are capable of sensing changes in the surrounding environment as a critical means to prevent crime and terrorism. In theory, "a smart container would include the means of detecting whether someone has broken into a sealed container and would have the ability to communicate that information to a shipper or receiver, via satellite or radio."[40]

Under this initiative, CBP provides selected importers with sensors to be secured inside a container. The sensors can detect whether or not a container has been entered during transit and will submit the information to CBP. The first phase

---

[37] Laser Visas are a type of visa that could also be used by citizens of Mexico to gain short-term entry (up to six months) for business or tourism into the United States.

[38] The International Civil Aviation Organization Technical Advisory Group, New Technology Working Group, *Biometric Deployment of Machine Readable Travel Documents*, Technical Report (Version 2.0), May 21, 2004.

[39] DOJ, DOS, and the NIST, Report to Congress, *Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents*, Jan. 2003.

[40] Daniel MacHalaba and Andy Pasztor, "Thinking Inside the Box: Shipping Containers Get 'Smart'," *The Wall Street Journal Online*, Jan. 15, 2004.

of 'smart box' testing involves volunteer importers with containers originating in Europe and Asia, moving through U.S. ports in New York-New Jersey, Los Angeles-Long Beach, Seattle and Charleston.[41]

Additional efforts to harden the border through the use of technology include the following (see **Appendix A** for a description of each program):

- Integration of Data Systems;
- Integrated Surveillance Intelligence System (ISIS);
- Operation Safe Commerce; and
- Unmanned Aerial Vehicles (UAV).

Efforts to Make the Border More Accessible for Legitimate Travel and Trade

The facilitation of legitimate cross-border travel and commerce, while still providing for adequate border security, has long been a challenge for policy makers. CBP inherited several initiatives aimed at using technology to help speed up the inspection processes for *low-risk* travelers and goods, which allows CBP inspectors to focus their attention on high-risk situations, as discussed below.

NEXUS/SENTRI

NEXUS and the Secure Electronic Network for Travelers' Rapid Inspection (SENTRI) are programs used at land ports of entry to facilitate the speedy passage of low-risk, frequent travelers. NEXUS is located at selected northern ports of entry while SENTRI is located at selected southwest ports of entry. Ports of entry are selected based on the following criteria: (1) they have an identifiable group of low-risk frequent border crossers; (2) the program will not significantly inhibit normal traffic flow; and (3) there are sufficient CBP staff to perform primary and secondary inspections. Travelers can participate in the program if: (1) they are citizens or legally permanent residents of the United States, citizens of Mexico or Canada, or legally permanent residents of Canada; (2) they have submitted certain documentation and passed a background check; (3) they pay a user fee; and (4) they agree to abide by the program rules.[42]

Both programs use an electronic identifier (e.g., a proximity card for NEXUS participants or a radio transponder for SENTRI participants) that triggers an automated system to review the Interagency Border Inspection System (a background check system) and other records related to the vehicle and its designated passengers once the vehicle enters the NEXUS or SENTRI lane. While NEXUS and SENTRI lanes are not at all land border crossings, efforts are underway to implement them at additional land border crossings.

---

[41] R.G. Edmonson, "United States launches 'smart box' testing," *The Journal of Commerce Online*, Nov. 20, 2003, accessed at [http://www.joc.com].

[42] See 8 CFR §286.8.

Free and Secure Trade

The Free and Secure Trade (FAST) program is a joint U.S.- Canada and U.S. - Mexico initiative that is aimed at expediting commerce across both the Southwest and the Northern border. FAST offers pre-approved importers, carriers, and registered drivers an expedited processing through land ports of entry. FAST is available to "low-risk" participants who have a demonstrated history of compliance with relevant legislation and regulations. Importers and carriers must be C-TPAT-certified in order to participate; carriers must also be approved as FAST Highway carriers; and drivers must possess a FAST Commercial Driver Card. In order for a shipment to be processed across the border as a FAST shipment, each of the parties involved must be FAST-certified, and less-than-truckload FAST shipments cannot be consolidated with non-FAST shipments and be processed through the FAST lanes at the border. While FAST lanes are not at all land border crossings, efforts are underway to implement them at additional land border crossings. FAST is also an harmonized clearance process, in that it operates in both directions across the Northern border (shipments exported from the United States into Canada can also be processed through the Canadian version of FAST: Partners in Protection).

Additional efforts to make the border more accessible for legitimate travel and trade include the following (see **Appendix A** for a description of each program):

- INS Passenger Accelerated Service System (INSPASS) and
- I-68 Canadian Border Boat Landing Program / Outlying Area Reporting Station (OARS)

In addition to technology used to facilitate legitimate travel and goods across the border by way of a vehicle, DHS also inherited programs designed to facilitate legitimate travel of certain groups of people. An example of such a program is the Visa Waiver Program, as discussed below, and the Laser Visa (Mexican Border Crossing Card). (See **Appendix A** for a discussion of the Laser Visa).

Visa Waiver Program (VWP)[43]

The VWP allows nationals from certain countries to enter the United States as temporary visitors for business or pleasure without first obtaining a visa from a U.S. consulate abroad.[44] By eliminating the visa requirement, this program facilitates international travel and commerce and eases consular office workloads abroad, but it also bypasses the first step by which foreign visitors are screened for admissibility to enter the United States. Travelers under the VWP do not need a visa, and thus no background checks are done *prior* to their arrival at U.S. ports of entry, which allows only one opportunity — immigration inspection at the port of entry — to identify inadmissable aliens. While this program facilitates travel, questions have been raised

---

[43] This section was taken from CRS Report RL32221, *Visa Waiver Program*, by Alison Siskin.

[44] The Attorney General in consultation with the Secretary of State, using criteria established by Congress, determines which countries may participate in the program.

about the VWP being a potential loophole for terrorists. Of concern to some is the delay in issuing nationals from the participating countries passports that contain biometric identifiers, although this concern may have abated since the Administration is now requiring foreign nationals entering the United States through the VWP to be enrolled in the U.S.-VISIT program.[45]

Strengthening the Border Through More Effective Use of Intelligence[46]

Intelligence plays an essential role in the protection of U.S. national security, one element of which is to contribute to the protection of U.S. borders. As with traditional foreign intelligence,[47] the primary role intelligence plays in the context of border security is to provide indications and warnings to government personnel responsible for border protection — primarily DHS personnel. Regardless of where the intelligence is collected — domestically or internationally — intelligence contributes to the protection of U.S. borders by seeking to prevent certain goods and individuals from crossing U.S. borders. However, as the tragic events of September 11, 2001, demonstrated, even when intelligence systems and mechanisms are in place to prevent individuals with inimical intent from crossing U.S. borders, it only takes one failure of the intelligence process and/or individuals involved in it, contribute to a potential catastrophe.[48] Traditional foreign intelligence as well as criminal intelligence contribute to enhancing border security.

At the most basic level, intelligence is designed to find where the danger lies. With respect to protection of the U.S. borders, the primary goal is to collect, analyze and rapidly disseminate intelligence that can deny entry into the United States of terrorists or dangerous material that could be used as a weapon by terrorists. With respect to terrorists, one of the most useful tools in the government's counterterrorism arsenal for border protection is the Terrorist Screening Database (TSDB) first compiled by the Terrorist Threat Integration Center.[49] As a testament

---

[45] While Congress set a deadline of Oct. 26, 2004 for all VWP countries to issue passports that contain biometric identifiers to their nationals in order to continue participation in the program, the deadline was moved back by one year due to concerns with respect to the time it would take for the countries to be able to meet the mandate.

[46] This section was written by CRS Specialist Todd Masse.

[47] Foreign intelligence is defined as "... information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence, except for information on international terrorist activities." See Part 3.4d, Executive Order 12333, "United States Intelligence Activities," Dec. 4, 1981.

[48] Both the *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Dec. 2002), and the *Final Report of the National Commission on Terrorist Attacks Upon the United States* (July 2004) found that there were various missed opportunities with respect to the lack of "watchlisting" of three of the 19 hijackers (Khalid al-Midhar, as well as brothers Salem and Nawaf al-Hazmi).

[49] Although it is now commonplace to hear public policy arguments about the integration (continued...)

to the robust role that traditional foreign intelligence entities are playing in the protection of border security, of the more than 20,000 records in the Terrorist Screening Database in 2004, the Central Intelligence Agency provided just over 42% of the entries, the State Department provided almost 42%, the National Security Agency provided 10%, the Federal Bureau of Investigation almost 4%, and the Defense Intelligence Agency just under 3%.[50] At the sensitive but unclassified (SBU) security level, the TSDB is then shared broadly across the U.S. government, to include agencies such as the DHS, the Federal Bureau of Investigation (and the FBI-led Terrorist Screening Center), the Department of Justice-led Foreign Terrorist Tracking Task Force[51]), the Department of Defense, as well as the Department of State, among others. A "hit" on the TSDB will trigger certain protective actions by the law enforcement, intelligence or security personnel having interaction with the individual.

With respect to protection against illicit cargo coming into the United States and the potential for shipping to be used as a conveyance of weapons of mass destruction, one of the unique tools being used by DHS's CBP is its Automated Targeting System. With shipments into the United States in the thousands of containers per day, it is not practically or financially feasible to inspect each container. Building on years of experience in interdicting drugs being shipped into the United States through cargo containers, DHS's CBP established the interagency — supported National Targeting Center (NTC) as a tool to triage and effectively target cargo containers for inspection. Working with the intelligence community and law enforcement community personnel, the NTC's Automated Targeting System develops dynamic rules and algorithms which allow it to examine a broad scope of passenger and cargo factors to assign appropriate risk scores. Certain risk scores flag a shipment or container for human inspection.

In short, intelligence serves as a force multiplier in contributing to the protection of U.S. borders. It serves the direct purpose of providing advance warnings to alert officials on the front lines of U.S. borders. However, its indirect use may be equally valuable. That is why domestic intelligence officials, including those at the state and

---

[49] (...continued)
of various terrorist watchlists, historically, there was one watchlist which had as its singular purpose, preventing known or suspected terrorists from entering the country. This watchlist, initiated by the U.S. Department of State's Bureau of Intelligence and Research (INR) in 1987 to assist the Bureau of Consular Affairs in making decisions about granting visas, was known as "TIPOFF." Pursuant to Homeland Security Presidential Directive-6, elements of the TIPOFF database have been transferred to the Terrorist Threat Integration Center (TTIC). In turn, TTIC and its databases will be incorporated in the new National Counter-Terrorism Center, which was statutorily created by P.L. 108-458.

[50] See Testimony of Russell E. Travers, Deputy Director for Information Sharing and Knowledge Development, the Terrorist Threat Integration Center, Before the National Commission on Terrorist Attacks Upon the United States, Washington, Jan. 26, 2004. These figures as of Jan. 8, 2004.

[51] The Terrorist Screening Center and the Foreign Terrorist Tracking Task Force have the dual mission of denying known or suspected terrorists entry into the United States and, should they gain entry to the United States, to locate, prosecute or deport any such aliens.

local levels, collect intelligence within their communities to put international terrorist activities into a local context. It is also why experts believe there needs to be a wide access to information that may not seem to be relevant in a national context, yet may prove what's happening in Sanaa, Yemen, may be directly or indirectly relevant and valuable to state and local law enforcement and intelligence personnel on the ground.

Multiplying Effectiveness Through Engagement of Other Key Actors in Enforcement[52]

While border security policies may not have received heightened attention until after the terrorists attacks, efforts to improve border management date back to 1995. For example, the United States and Canadian governments entered into a joint accord on February 24, 1995 called *Our Shared Border*. The 1995 accord brought together five agencies (the former United States INS, the former U.S. Customs Service, Revenue Canada, Citizenship and Immigration Canada, and the Royal Canadian Mounted Police) to focus on joint border issues such as enhancing security through more effective inspection efforts that target specific problem areas (e.g., drugs, and smugglers), and the continued commitment to pool inspection and enforcement resources. And in 1999, the two countries entered into a partnership, *Canada-U.S. Partnership Forum* (CUSP). CUSP provided a mechanism for the two governments, border communities and stakeholders to discuss issues of border management. The guiding principles for U.S.-Canada cooperation resulting from these dialogues are as follows:

- Streamline, harmonize and collaborate on border policies and management;
- Expand cooperation to increase efficiencies in customs, immigration, law enforcement, and environmental protection at and beyond the border; and
- Collaborate on common threats from outside the United States and Canada.

Current bilateral efforts include a declaration signed on December 12, 2001, by the United States and Canadian governments establishing a "smart-border." The declaration included a 32-point plan to secure the border and facilitate the flow of low-risk travelers and goods through the following:

- Coordinated law enforcement operations (i.e., IBETS, see **Appendix A**);
- Intelligence sharing;
- Infrastructure improvements;
- The improvement of compatible immigration databases;
- Visa policy coordination;

---

[52] Programs and policies discussed under other headings or listed in **Appendix A** are also examples of multiplying effectiveness through the engagement of other actors (see for example, *preinspections, CCP, CSI, C-TPAT, FAST, IBETS, ISI,* and *NEXUS*).

- Common biometric identifiers in certain documentation;
- Prescreening of air passengers;
- Joint passenger analysis units; and
- Improved processing of refugee and asylum claims, among other things.

On December 3, 2001, the two countries signed a joint statement of cooperation on border security and migration that focused on detection and prosecution of security threats, the disruption of illegal migration, and the efficient management of legitimate travel.

In March 2002, the United States and Mexico announced a partnership to create a new, technologically advanced "smart border" to assure tighter security while facilitating legitimate travel. The U.S.-Mexico Border Partnership Action Plan has 22 points that include greater cooperation between the two governments in order to better secure border infrastructure and facilitate the flow of people and goods between the countries. The plan also calls for the development of integrated computer databases between the two countries and express lanes at high volume ports of entry for frequent, pre-cleared low-risk travelers.[53]

In addition to the bilateral agreements between the U.S./Canada and the U.S./Mexico, the United States has begun working with the European Union (EU) to facilitate cooperation on the CSI, as discussed above. On November 18, 2003, the United States and EU signed an agreement that would facilitate such cooperation by establishing an EU-wide container security policy.[54]

The Construct Illustrated Using Selected Programs

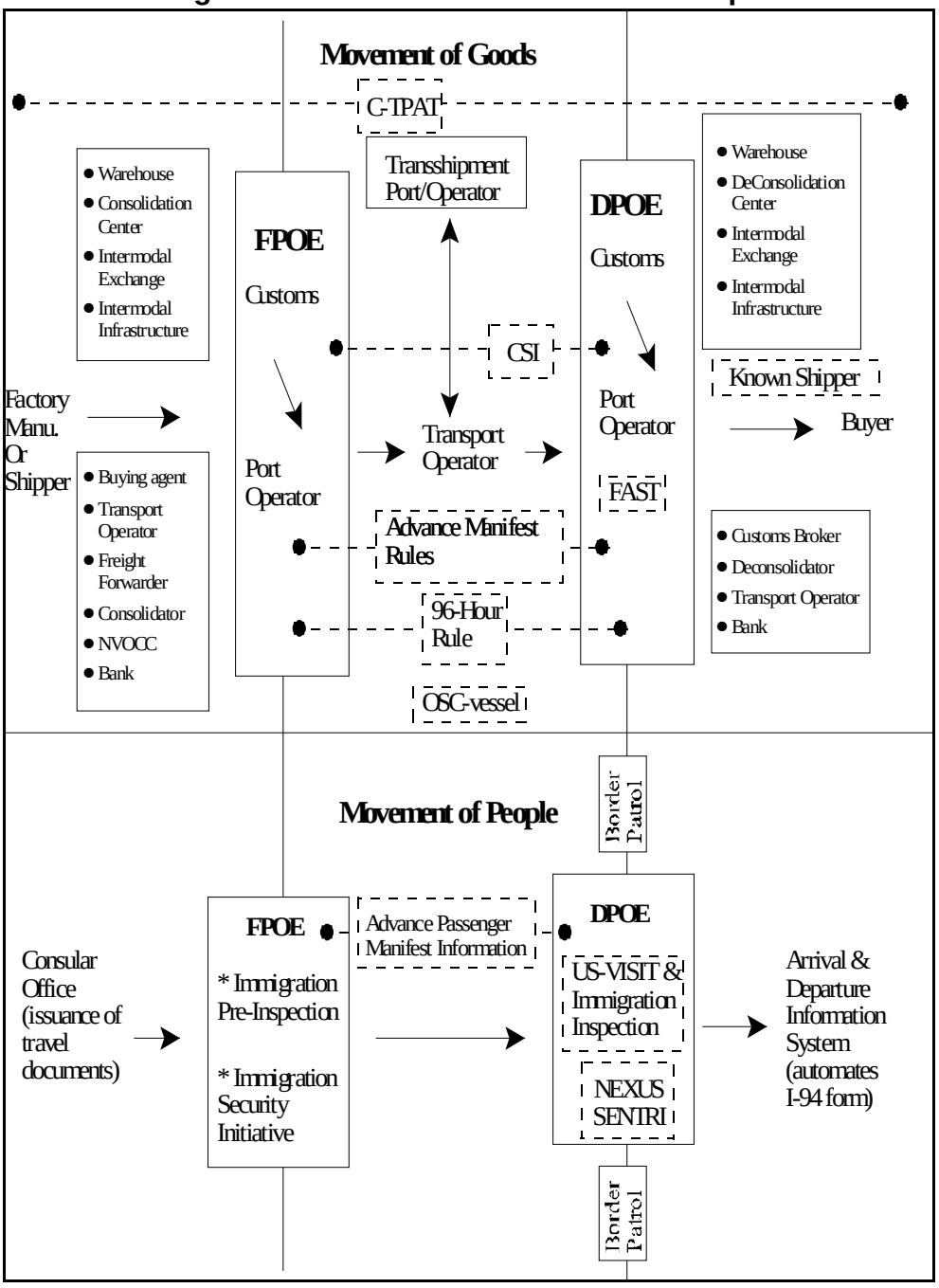
Figure 1 maps some of the current policy approaches discussed in this report. For example, illustrations of "pushing the border outward" in order to intercept unwanted people and goods before they reach the United States include CBP's and FDA's advance manifest rules; the Coast Guard's 96-hour rule; the CSI; and passenger pre-inspection at foreign airports. Examples of "making the border more accessible for legitimate travel and trade" include the C-TPAT; FAST; and the NEXUS/SENTRI trusted traveler/frequent crosser programs. Examples of "multiplying effectiveness through the engagement of other actors" include C-TPAT; CSI; FAST; NEXUS; and passenger pre-inspection.

---

[53] See [http://www.whitehouse.gov/infocus/usmxborder/22points.html].

[54] Intellibridge Global Intelligence Solutions, "EU, United States Announce Agreement to Facilitate Cooperation on Container Security," *Homeland Security Monitor*, Nov. 19, 2003; and BNA, "EU, United States Reach Commitment to Establish Security Standards for Trans-Atlantic Freight," *International Trade Reporter*, vol. 20, no. 47, Nov. 27, 2003.

Figure 1. Movement of Goods and People



Source: CRS and CRS analysis of OECD figures in *Security in Maritime Transport*.
Note: FPOE = foreign port of exit, and DPOE = domestic port of entry.

Conclusion

Balancing security with trade and travel may require a "layered approach" to attain both goals. The next report in this series, *Border and Transportation Security: Possible New Directions and Policy Options*, examines the concept of layering and how it may fit into BTS. The current programs and policies in place, however, do reflect some layering. For example, the framework set forth in this report highlights the purposeful *overlapping* of programs and policies in order to attain BTS. *Efforts to push the border outwards* are aimed at preempting potential attacks and preventing individuals who are trying to surreptitiously enter the United States. The various preinspections and advance passenger/cargo notice programs were developed with this in mind. If someone, however, is able to penetrate the first layer of security then *efforts to harden the border* are put to the test. The use of biometric identifiers in travel documents and smart containers for the shipment of goods are both examples of how technology is being used to harden the border. In addition to *efforts to harden the border*, the use of *intelligence* and *engaging other actors* such as state and local law enforcement and our foreign neighbors are other cumulative measures that have been taken to attain better BTS.

While the programs and policies highlighted in this report may reflect an attempt at layering, some contend that there are still gaps in the system.[55] The current programs and policies were either put into place as a result of the 9/11 terrorist attacks or predated the attacks. Those programs and policies that were put into place as a result of the attacks were done so with a sense of urgency — *to prevent another attack*. Programs and policies already in existence prior to the attacks, however, were created with a different focus and not necessarily with the goal of keeping terrorists out of the country. As will be examined in the next report, current efforts to provide a layered approach to BTS would mean applying some measures of security effort to almost every point of vulnerability or opportunity.

As noted earlier, this report is one of a series of three CRS reports that address the issue of BTS. The first report in the series, CRS Report RL32839, *Border and Transportation Security: The Complexity of the Challenge*, analyzes the reasons why BTS is so difficult to attain. This report is the second in the series. The final report is CRS Report RL32841, *Border and Transportation Security: Possible New Directions and Policy Options*.

---

[55] See for example, Stephen Flynn, *America The Vulnerable: How Our Government Is Failing to Protect Us From Terrorism* (New York, N.Y.: HarperCollins Publishing), 2004.

Appendix A: Selected Additional BTS Programs

Carrier Consultant Program (CCP). Sometimes referred to as prescreening, the CCP was originally developed in the former INS. Working with officials from the Department of State, CBP deploys officers to work with air carriers to preempt attempts to use those carriers to gain illegal entry into the United States using fraudulent documents. In doing so, CCP officials work towards eliminating the arrival of improperly documented aliens at a U.S. port of entry prior to their departure from the foreign port. At domestic airports, CCP officials work with airlines in identifying any illegal or suspect activity involving the carrier, primarily related to the use of fraudulent documents. While the goal of CCP is to reduce illegal migration, the program has received heightened attention in this post 9/11 era.

I-68 Canadian Border Boat Landing Program/Outlying Area Reporting Station (OARS). The I-68 Canadian Border Boat Landing Program permits enrolled participants admission to the United States by small pleasure boats without an inspection. The program requires applicants[56] to appear in person for an inspection and interview. During the inspection/interview process, applicants names are checked against the IBIS and biometrics are collected. Upon approval, participants are issued a boating permit for the season that allows them to enter the United States from Canada without submitting to an inspection.

OARS allows travelers of small boats who are not in possession of a valid I-68 form to enter the United States via Canada without presenting themselves for inspections. Travelers can use one of the 33 OARS videophone stations upon entry into the United States.[57] The stations are located at public marinas along the Canadian border and provide automated inspections through a two-way visual and audio communication between the person and the remote inspector.

Immigration Security Initiative (ISI). Like CCP, ISI was originally developed in the former INS. CBP is now piloting ISI at several foreign airports. ISI relies on CBP inspectors positioned at foreign airports to intercept people who have been identified as national security threats from traveling to the United States ISI has been compared to CBP's CSI, discussed above, which targets high risk containers for inspections.

Integrated Border Enforcement Teams (IBETS). IBETs are bi-national, multi-agency law enforcement teams that target cross-border criminal activity. Although IBETS were originally created in 1996 along the British Columbia and Washington state border to target cross-border crimes that usually involved illicit drug violations, the terrorist attacks have prompted officials in both countries to expand IBETs role to include counterterrorism measures.

---

[56] U.S.-Canadian citizens, legal permanent residents of the United States or landed immigrants of Canada can participate in the program.

[57] The phones are two-way visual and audio between the inspector and the applicant for admission.

INS Passenger Accelerated Service System (INSPASS). INSPASS is used at selected international airports.[58] It is a form of pre-inspections for low-risk, frequent travelers.[59] INSPASS records a biometric geometry (of the hand) for each enrollee that is verified when the traveler inserts his card. Upon arrival at an airport that has INSPASS, enrollees proceed to an INSPASS kiosk where they access an automated hand geometry reader. Upon approval by the kiosk, the traveler receives a receipt of his inspection. INSPASS applicants must enter the United States on certain nonimmigrant visas[60] or under the Visa Waiver Program.[61]

Integration of Data Systems. CBP officials use several data systems and databases that assist them with identifying aliens who are potentially inadmissible under the Immigration and Nationality Act or otherwise may pose a threat to the country. CBP officials also utilize several data systems and databases with respect to identifying high-risk commercial goods that warrant further inspection or review. Of concern are the numerous data systems and databases that are not integrated or not readily accessible. Critical to the success of border security is the ability to process information in real time.

The legacy Customs Service and now CBP have been engaged in a long-term effort to develop a new automated system to process and track the entry of all goods into the country. The Automated Commercial Environment (ACE) will utilize web-based electronic accounts to provide information regarding cargo inspections, status of clearance and other information to CBP and account users.

Integrated Surveillance Intelligence System (ISIS). Along the northern and southwest borders, the border patrol uses ISIS as a surveillance tool. ISIS is comprised of remote video surveillance cameras that are mounted on top of towers, which are remotely monitored. According to CBP, "one camera uses natural light and takes traditional video images; the other uses 'infrared' imaging for night vision."[62] ISIS also consists of sensors and an Integrated Computer Assisted Detection (ICAD) database.

Known Shipper Programs. The Transportation Security Administration uses a program that differentiates trusted shippers that are known to a freight forwarder or air carrier through prior business dealings, from unknown shippers.

---

[58] According to CBP, "INSPASS is currently operational at six international airports: Los Angelas, CA; Newark, NJ; JFK, NY; Washington-Dulles, VA; and the U.S. preclearance sites at Vancouver and Toronto in Canada," [http://www.cbp.gov/linkhandler/cgov/travel/frequent_traveler/inspass.ctt/inspass.doc].

[59] Citizens of the United States, Canada, Bermuda, and participants in the Visa Waiver Program who travel to the United States on business three or more times a year, or are diplomats, representatives of international organizations, or airline crew members from VWP countries are eligible to enroll in INSPASS.

[60] B-1 (visitor for business), E-1 (treaty trader), E-2 (treaty investor) or L-1 (intra-company transferee).

[61] See CRS Report RL32221, *Immigration: Visa Waiver Program*, by Alison Siskin.

[62] See [http://www.cbp.gov/xp/CustomsToday/2003/august/cameras.xml].

Under such a program, shipments from unknown sources are identified and placed under closer scrutiny.[63]

Laser Visa (Mexican Border Crossing Card). Mexican nationals applying for admission to the United States as visitors are required to obtain a visa or hold a Mexican Border Crossing Card, now referred to as the "laser visa." The laser visa is used by citizens of Mexico to gain short-term entry (up to six months) for business or tourism into the United States. It may be used for multiple entries and is good for ten years. Under current practices, Mexican nationals in possession of a laser visa will be exempt from the requirements of the U.S.-VISIT program, thus allowing for a speedy passage into the United States.

North American Security Perimeter. As the United States moves forward with implementing much of the security requirements in the PATRIOT Act and the Border Security Act, many fear that the tighter security requirements will impede the flow of people across the border. Some critics are advocating for a more open border. The ideal of a North American Perimeter Security concept has been around for several years and the basic premise of a North American Perimeter Security would move inspections and enforcement activities away from the border. Such a concept would essentially eliminate barriers to the movement of people (and goods) across the shared border. P.L. 107-173 called for a study to examine the feasibility of establishing a North American Perimeter Security program that would provide for increased cooperation with foreign governments on questions related to border security. The North American Perimeter Security, however, would require the harmonization of United States and Canadian immigration and refugee policies, among other things. While such a harmonization of policies may be problematic following the events of 9/11, both countries have begun to harmonize other policies at incremental levels that could be viewed as "pushing the border out" (i.e., preinspections and reverse inspections).

Operation Safe Commerce (OSC). OSC is a pilot program that brings together private businesses, the maritime industry and the government to analyze security procedures and practices for cargo entering the country and develop improved methods for securing the supply chain. OSC's goal is to protect the global supply chain while facilitating the flow of commerce by identifying potential supply chain security weaknesses.

Unmanned Aerial Vehicles (UAV). In 2004 DHS launched an initiative, dubbed the Arizona Border Control (ABC) Initiative that uses technology such as the UAV to increase border surveillance along the Arizona/Mexico border. Currently, the border patrol is piloting two UAVs along the Arizona and Mexico border.

---

[63] See CRS Report RL32022, *Air Cargo Security*, by Bartolomew Elias.